AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, FBI Task Force Officer Brett Fernald, depose and state as follows:

AGENT BACKGROUND

1. I am a Task Force Officer with the Federal Bureau of Investigations (FBI), and have held this title since I was assigned to the Special Enforcement Division in June 2019. My duties and responsibilities as a Task Force Officer include investigating and supporting operations involving national security matters and federal criminal violations that include international and domestic terrorism, crimes against children, narcotics, and other criminal violations. I am also a Police Officer with the city of Manchester, NH and have been so employed since April 2013. I have been assigned to the Manchester Police Department ("MPD") as a Detective since August of 2016. Prior to my employment with MPD, I was a Police Officer for the town of Hooksett, NH from December 2010 until April 2013. I graduated from the New Hampshire Police Standards and Training Class 154 in April 2011. I have received training from the Manchester Police Department in-house training academy and the New Hampshire Police Standards and Training full-time police academy. I have also attended numerous training courses covering many different aspects of investigations. Prior to joining the Hooksett Police Department in 2010, I served honorably in the US Army from 2006 to 2010.

2. Throughout my career, I have led and/or been involved with investigations of homicides, sexual assaults, robberies, assaults, burglaries, arsons, and other serious crimes.. My investigations have included the use of the following investigative techniques: physical surveillance; handling of cooperating sources and witnesses; exploitation of cellular, social media, and Internet Protocol ("IP") based communications data; execution of search and seizure warrants; and the execution of arrest warrants.

3. Based on my training, experience, and information provided to me by other law enforcement officers, I am familiar with the modus operandi used by individuals engaged in the violation of various criminal offenses, such as those related to acts of violence and firearms. For example, I have handled many cooperating sources and witnesses who have provided information to me specifically related to various firearms offenses and violent crimes. Many of these investigations have resulted in the execution of search warrants, arrest warrants, and eventual convictions.

PURPOSE OF AFFIDAVIT

4. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement's possession and are further described in Attachment A, and the extraction for that property of electronically stored information described in Attachment B.

5. The property to be searched is the following (hereafter, collectively, the "**Target Devices**"):

a. Black Apple iPhone seized by law enforcement in Manchester, NH on June 29, 2022 from David Berard (hereafter, "the Black iPhone").

b. Silver/Black Alienware Model P816 Laptop computer, serial number 8XCWQF2, seized by law enforcement in Manchester, NH on June 29, 2022 from David Berard (hereafter, "the Alienware Laptop")

Each of the Target Devices is secured at FBI Boston, Bedford Resident Agency, located at 15 Constitution Drive, Bedford, NH 03110.

6. Based on the information contained herein, there is probable cause to believe that the **Target Devices** contain evidence, fruits, and instrumentalities of the crimes of Title 18 U.S.C.

§ 875(c) [Threatening Interstate Communications] and 18 USC 922(a)(6) [False Statement Made to a Dealer in Acquisition of a Firearm].

7. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, and information received from other law enforcement officers. I have not set forth every detail I or other law enforcement officers know about this investigation but have set forth facts that I believe are sufficient to evaluate probable cause as it relates to the issuance of the requested warrant.

8. The applied-for warrant would authorize the forensic examination of the Target Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

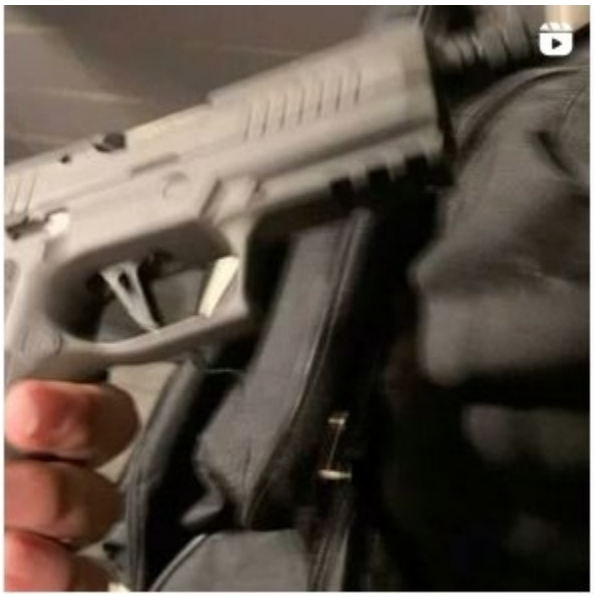
PROBABLE CAUSE

9. On June 27, 2022, a resident of Los Angeles, CA submitted an online tip to the FBI National Threat Operations Center (NTOC) via tips.fbi.gov that an Instagram user "thedavidyouloved" had sent a message threatening to commit mass violence. The resident reported to the FBI that a message was posted by "thedavidyouloved" to the account of her daughter, who is also a California resident. The message appears to have been posted on June 25, 2022.

10. Below is a screenshot captured of the content of the posted message:

11. The Instagram account that was associated with "thedavidyouloved" also showed pictures of firearms and a video of a male subject pointing two firearms at a mirror, which were posted within short temporal proximity—approximately one day—to the posting of the threatening message. The male subject in the video posted to Instagram on June 26, 2022 is seen with two separate firearms pointed into a mirror while he makes statements including "this is what I got for you bitch ass nigga, right there in the dick hole, I'm gonna shoot the dick right off."

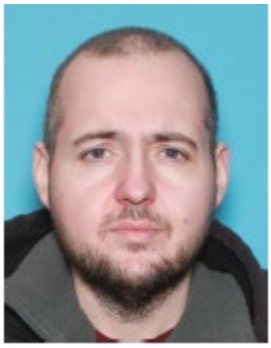
12. Below are screen shots taken from the posts:



13. On June 27, 2022, law enforcement sent a preservation request and emergency voluntary disclosure request to Meta (the parent company of Instagram) for information regarding the user "thedavidyouloved". Later that day, law enforcement received information from Meta that the subject associated with the account was David BERARD, date of birth [redacted]1984. The telephone number associated with the account is [redacted]6863 and the IP address associated with the account is [redacted] and came back to Boston, MA.

14. An "Officer Safety" warning from the New Hampshire Information and Analysis Center (NHIAC) circulated later on June 27, 2022 warned officers of BERARD's threat, and advised that BERARD's last known address was at the [redacted]). However, the bulletin also advised that BERARD had recently obtained a New Hampshire Driver's License on June 22, 2022.

15. Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") personnel conducted a query of BERARD through the Criminal Justice Information System, and confirmed that on June 22, 2022, BERARD was issued a New Hampshire driver's license [redacted]). On that license, BERARD listed his address as [redacted], Manchester, New Hampshire. Below is the photograph associated with that license:



16. ATF Special Agent John Cook contacted the Manchester Firing Line, a federally licensed firearms dealer, and requested a search for any purchases made by BERARD. Manchester Firing Line advised that on June 23, 2022, BERARD purchased the following three (3) firearms:

a. Sig Sauer model P320 X-Carry 9mm pistol (Serial Number 58J328181)

b. Glock model 43X 9mm pistol (Serial Number BXCL871)

c. Colt M4 5.556 rifle (Serial Number CR718204)

17. When purchasing the firearms, BERARD completed an ATF Form 4473. On that form, BERARD listed his residence as 55 S. Main Street Manchester, New Hampshire.

18. On June 28, 2022, ATF Special Agent John Cook spoke to management at [redacted], Manchester, New Hampshire. Management at that location advised that BERARD applied many years ago—on June 30, 2012—to live at the location, but never did reside there. On June 29, 2022, a detective of the Manchester Police Department spoke to a resident at [redacted], who said that she had allowed BERARD to stay overnight at her residence as a guest for one night roughly two weeks prior because she believed him to be homeless, but she has not permitted him to stay there since.

19. Additionally, on June 27, 2022, I had contacted the residents of 33 Ahern Street Manchester, New Hampshire. That resident advised that they do not know David BERARD and that he does not reside at [redacted] Manchester, New Hampshire.

20. Boston Police advised that David BERARD is believed to be homeless and living in the Boston area. Boston Police Department Detective Luis Anjos advised that security officers at the Boston Health Care for the Homeless Program (780 Albany Street Boston, MA) reported that BERARD has been repeatedly seen in the area. Additionally, the Night Desk Supervisor at the [redacted], advised on June 27, 2022 that she recognized BERARD but that he had not stayed at the shelter for the last two-to-three weeks.

21. Due to the nature of Berard's message and purchase of firearms, the Boston Regional Information Center began to "ping" his last known phone number. That phone number was the same as the number associated with the Instagram account for "thedavidyouloved." Pinging this phone number and other investigative methods led law

enforcement to locate BERARD, who had a phone on his person (the Black iPhone), at a shopping center at 30 March Ave. in Manchester, NH on June 29, 2022. The male subject seen in the video of "thedavidyouloved" matched the appearance of BERARD.

22. Upon making contact with BERARD, he was initially transported to Elliot hospital for an involuntary hospital admission. BERARD was in possession of the Black iPhone (the only phone in his possession), the Alienware Laptop, and several bags containing his belongings at the time he was to be transported to the hospital. David Berard was also in possession of three firearms, two of which were handguns and matched the description of the firearms seen on his Instagram page, "thedavidyouloved." He was also in possession of various types of ammunition. His belongings were taken by law enforcement for safe keeping. He was subsequently arrested by ATF agents at the hospital on probable cause for a charge of violating 18 USC 922(a)(6) [False Statement Made to a Dealer in Acquisition of a Firearm], based on the false residence that he stated on ATF Form 4473, which he used to purchase the three firearms from Manchester Firing Line.

23. Instagram may be accessed by smartphones and computers via the Internet. The disclosure provided by Meta indicates that the threatening message sent by "thedavidyouloved" was transmitted by an electronic device linked to a T-Mobile account. I know from my experience and research that T-Mobile is a telecommunications company. The disclosure from Meta therefore indicates that the threatening message posted to Instagram was transmitted by a phone.

24. I believe there is probable cause that the Target Devices may contain evidence including, but not limited to, the following: BERARD's knowledge of, or affiliation with, the

recipient of the threatening Instagram message; account information, or personally-identifying information of the recipient of the threatening Instagram message; Instagram or other social media registrations; the videos and/or photos of BERARD posted to Instagram; other threats BERARD made on social media or in other electronic communications; the specific handles and phone numbers discussed herein; and/or evidence of where BERARD resides (supporting that his stated address on ATF Form 4473 in the purchase of firearms is false). Therefore, probable cause exists that evidence of BERARD's criminal activity—threatening interstate communications as well as his false statement on the ATF Form 4473—is contained on the Target Devices.

25. The Target Devices are currently in storage at FBI Boston, Bedford Resident Agency located at 15 Constitution Drive, Bedford, NH 03110. In my training and experience, I know that the Target Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Target Devices first came into the possession of law enforcement.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call

log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media.

Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data

and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that many smartphones like the Black iPhone (included in Attachment B's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Based on my training, experience, and information provided to me by other law enforcement personnel, I am aware that individuals commonly store records of the type described in Attachments B in mobile phones, computer hardware, computer software, and storage media. As evidence both of the crimes and of who used the device can be located in essentially any part of the cellular telephone, it is necessary to search an entire phone, including any applications, to locate the evidence discussed herein.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. Regarding the Alienware Laptop, there is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

h. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

i. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

j. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

k. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Furthermore, on computers such as the Alienware Laptop, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. Based on the information described above, I believe BERARD made interstate threats and that he illegally acquired the firearms seized from him within the District of New Hampshire. Based on the information contained herein, I believe the **Target Devices** will likely contain evidence of those violations.

34. Therefore, I have probable cause to believe that evidence, fruits, and instrumentalities of the crimes of Title 18 U.S.C. § 875(c) [Threatening Interstate Communications] and 18 USC 922(a)(6) [False Statement Made to a Dealer in Acquisition of a Firearm] are contained on the Target Devices. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Target Devices described in Attachment A to seek the items described in Attachment B.

/s/ Brett Fernald
Brett Fernald, Task Force Officer
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: _____
Time: _____

_____
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of Property to Be Searched

The property to be searched consists of the following (collectively, the "Target Devices"):

a. Black Apple iPhone seized by law enforcement in Manchester, NH on June 29, 2022 from David Berard.

b. Silver/Black Alienware Model P816 Laptop computer, serial number 8XCWQF2, seized by law enforcement in Manchester, NH on June 29, 2022 from David Berard.

The Target Devices are currently secured at the FBI Boston, Bedford Resident Agency located at 15 Constitution Drive, Bedford, NH 03110.

This warrant authorizes the forensic examination of the Target Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of Information or Items to Be Seized

I. All records on the Target Devices described in Attachment A, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of Title 18 U.S.C. § 875(c) [Threatening Interstate Communications] and 18 USC 922(a)(6) [False Statement Made to a Dealer in Acquisition of a Firearm] and involve David Berard since January 1, 2022, including but not limited to:

A. Evidence of who used, owned, or controlled the equipment;

B. Evidence of the user's past whereabouts, and past and current place of residence;

C. Evidence of the user's Instagram registrations or other social media registrations;

D. The identities and aliases of David Berard;

E. The methods of communication used by individuals engaged in the violations listed above, including the telephone numbers, messaging applications, and social media accounts used by the individuals;

F. Evidence of David Berard's knowledge of, or affiliation with, the recipient of the threatening Instagram message;

G. Account information, or personally-identifying information of the recipient of the threatening Instagram message;

H. Videos and/or photos posted to Instagram from the equipment;

I. Evidence of threats David Berard made on social media or in other electronic communications;

J. Any information related to sources of guns (including names, addresses, phone numbers, or any other identifying information);

K. Types, amounts, and prices of guns purchased or sold as well as dates, places, and amounts of specific transactions;

L. All bank records, checks, credit card bills, account information, and other financial records;

M. The locations where evidence or other items related to the violations listed above was obtained, is stored, or has been discarded;

N. The substance of communications regarding the planning, execution, transactions, and/or discussions of the violations listed above;

O. The substance of communications regarding the acquisition or disposal of items involved in the violations listed above;

P. The substance of communications regarding firearms and interstate threats;

Q. The substance of communications regarding money, vehicles, communications devices, or other items acquired during or for activity that would result in the violations listed above;

R. Photographs of items or information related to the violations listed above;

S. The relationship between the users of the equipment;

T. The identity, location, and travel of users of the equipment;

U. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

V. Evidence of the attachment of other hardware or storage media;

W. Evidence of counter-forensic programs and associated data that are designed to eliminate data;

X. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

Y. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media; and

Z. Records relating to the ownership, occupancy, or use of the location from which the equipment was obtained by law enforcement investigators.

II. Evidence of user attribution showing who used or owned the Target Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history

III. Serial numbers and any electronic identifiers that serve to identify the equipment.

DEFINITIONS

For the purpose of this warrant:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying

information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.